修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　電気通信学研究科　情報通信工学専攻　博士前期課程		
氏　　名	阿部　功	学籍番号	0830002
論 文 題 目	非 CPC 型 LDPC 符号化の提案と それを用いた音楽電子透かし方式の自己同期復号		

要　旨

シンボルの挿入誤りや，削除誤りからなる同期誤りが生じる通信路において，誤りの発生箇所以降の全ての符号系列にずれが生じるため，受信側で符号語の区切りに相当する個所を正しく検出し，誤りを訂正する必要がある．

そのような同期問題の一例として，クリッピング(clipping，クロッピング，cropping) 攻撃による，連続した透かしデータの削除が起こるような状況での電子透かしが挙げられる．しかし，電子透かしは，様々な攻撃により雑音が多く生じ，かつ，抽出において誤り訂正符号(error correcting code, ECC)が利用される．そこで，反復符号を利用することで，SNR(signal-to-noise ratio) を向上させることが重要である．

本研究では，同期用ヘッダや CPC(Cyclically Permutable Codes) 性のない LDCP 符号を用い，復号において符号のハミング距離の特性から同期外し攻撃となるクリッピング攻撃への耐性を持たせる，自己同期復号-抽出アルゴリズムを提案した．また，このアルゴリズムは符号長に比例する計算量がかかってしまう問題を解決する，適応的高速復号アルゴリズムも提案した．これにより，埋め込みビット数の減少による電子透かしを埋め込むことによるデータの品質低下を小さくし，また，誤り訂正能力の高い符号を利用することを実現した．

同時に，本研究では，同期へのアプローチとして，符号の“ CPC 距離”という定義を行う．これにより，任意の符号に対して列置換による符号のパーミュテーションを行うことにより，符号に関わらず巡回性を内在する符号の CPC 性を持たせることを実現した．